

Adding control to arbitrary unknown quantum operations

Xiao-Qi Zhou,¹ Timothy C. Ralph,² Pruet Kalasuwan,¹ Mian Zhang,^{1,3}
Alberto Peruzzo,¹ Benjamin P. Lanyon,⁴ and Jeremy L. O’Brien^{1,*}

¹*Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of
Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom*

²*Department of Physics and Centre for Quantum Computation and
Communication Technology, University of Queensland, Brisbane 4072, Australia*

³*School of Applied and Engineering Physics, Cornell University, Ithaca, NY 14853*

⁴*Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, 6020 Innsbruck, Austria*

While quantum computers promise significant advantages, the complexity of quantum algorithms remains a major technological obstacle. We have developed and demonstrated an architecture-independent technique that simplifies adding control qubits to arbitrary quantum operations—a requirement in many quantum algorithms, simulations and metrology. The technique is independent of how the operation is done, does not require knowledge of what the operation is, and largely separates the problems of how to implement a quantum operation in the laboratory and how to add a control. We demonstrate an entanglement-based version in a photonic system, realizing a range of different two-qubit gates with high fidelity.

Perhaps the most promising future application of quantum science is quantum information processing, which promises secure communication¹ and greatly increased speeds for solving certain problems such as database searching², factoring³ and quantum simulation⁴. The excitement surrounding quantum computers lies in the fact that the number of elementary operations that they require to solve these problems scales only polynomially with the size of the input, in contrast to exponential scaling on a conventional computer. However, even a polynomial scaling of quantum computational resources still presents an enormous obstacle to practical realization. It may well be that although a quantum computer could in principle efficiently solve these important problems, it will remain practically infeasible to build one that can implement a sufficient number of operations, on enough qubits and with sufficient precision, to do anything useful. This motivates developing methods to reduce the resource overhead required to implement key quantum algorithms.

Quantum algorithms rely on the decomposition of a functional quantum circuit into an elementary logic gate set, such as that formed by single-qubit and two-qubit controlled-NOT (CNOT) gates⁵; there have been several experiments to demonstrate universal quantum gate sets in different physical architectures⁶ including ion traps^{7,8}, linear optics^{9–13}, superconductors^{14,15}, and atoms^{16,17}, and even small-scale algorithms^{18–21}. However, the large number of elementary gates required to implement even modest sized circuits presents a significant challenge. This complexity is due not only to the sheer number of elementary operations required but also the structure in which these gates are combined.

Controlled-unitary (CU) gates are a particularly important class of circuits, where one “control” qubit turns on or off a unitary operation U acting on a register of “target” qubits (Fig. 1a). These circuits features heavily in Kitaev’s phase estimation algorithm²² which underpins Shor’s factoring algorithm³ and quantum simulation⁴. In the context of quantum simulation, U could represent a simulation of the time-evolution operator of some physical system and the ability to add control qubits allows energy eigenvalues to

be read out via the phase estimation algorithm²³. Phase estimation is also a fundamental tool in quantum metrology. However, the current standard method of realizing CU gates, which relies on the decomposition of U into an elementary gate set, may not be suitable for these applications: in Kitaev’s phase estimation algorithm U may be an unknown “black box” which cannot be decomposed at all.

Here we present and demonstrate a simple method for realizing controlled quantum operations (CO), of which CU gates are a subset. In the following we first explain the technique in a way that is independent of any particular physical system, before describing a conceptual example in a photonic system. We then show that the equivalent operation can be achieved by exploiting an entangled initial state—reminiscent, but distinct from, cluster state quantum computing^{24,25}. Finally, we apply this approach in a series of proof-of-principle experiments implementing various two-qubit gates which include a CNOT, a number of other CU gates, as well as “entanglement filter” and “entanglement splitter” gates.

Results

Explanation of the general technique. Our approach for adding a control qubit to an arbitrary quantum operation O is shown conceptually in Figure 1b. In summary, conditional on the logical state of the control, the quantum state of the target register (ψ) is temporarily shifted into a part of an extended Hilbert space on which O does not act (imparts the identity operation). In this way the evolution of ψ is dependent on the control qubit state: if it is $|0\rangle$ ($|1\rangle$) then $\psi \rightarrow \psi$ ($\psi \rightarrow O\psi$). The Hilbert space is extended by employing an extra two levels in each quantum information carrier in the target register, making each a four level system with logical states $|0\rangle, |1\rangle, |2\rangle$ and $|3\rangle$. The action of each X_a gate is to swap information between the bottom two ‘qubit’ levels ($|0\rangle, |1\rangle$)

and the expanded Hilbert space ($|2\rangle, |3\rangle$) i.e.

$$X_a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (1)$$

$$\begin{aligned} X_a|0\rangle &= |2\rangle, & X_a|1\rangle &= |3\rangle \\ X_a|2\rangle &= |0\rangle, & X_a|3\rangle &= |1\rangle \end{aligned} \quad (2)$$

In spite of its conceptual simplicity, the technique has significant practical benefits: it largely separates the experimental problems of how to implement any given quantum operation in the laboratory and how to add a control qubit. This is relevant in many experimental cases where it is not at all clear how to directly add a control to a quantum operation, for example when O can be realized in analog fashion by turning on an experimental hamiltonian, or when O is a non-unitary operation implemented by directly coupling to a bath. Even in the case where O can be constructed with a universal gate set, the number of additional operations required to add a control will generally be far less following our approach. Furthermore, in situations where O is unknown our method may be the only way to add control. This is relevant in quantum metrology where the goal is to measure properties of O .

The method can be straightforwardly extended to realize the conditional implementation of two different operations O_1 or O_2 based on the state of the control qubit. Here, while the component of the state that is unmoved undergoes O_1 , the component of the state moved into the expanded Hilbert space undergoes O_2 . A further extension would be to add multiple control qubits to implement one of several quantum operations, based on the state of all of the control qubits. For example with two control qubits four operations O_1, O_2, O_3 , or O_4 could be implemented depending on the state of the control qubits.

An alternative approach to extending the Hilbert space would be to use another register of qubits and controlled-swap operations to move information between the registers. However, while adding more qubits has proved to be a significant experimental challenge, multi-dimensional quantum information carriers are readily available in most physical systems currently being investigated or used for quantum information processing. Trapped ions systems, for example, offer a large number of precisely controllable internal electronic and external vibrational degrees of freedom. Our technique could be implemented by conditionally moving quantum information between different electronic transitions, on which subsequent operations do not operate, or operate differently, on.

We note that in previous work it was shown how moving part of the state of a target qubit into an expanded Hilbert space can simplify adding control qubits²⁶. However, this only works in the case where the target is a single-qubit unitary and is at the expense of changing how the unitary must be implemented.

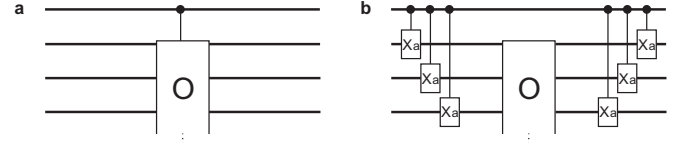


FIG. 1: Controlling arbitrary quantum operations using additional degrees of freedom. (a) Logic circuit in which quantum operation O is implemented on a register of qubits (target register), conditional on the logical state of a single control qubit. (b) Our approach to implementing the circuit in (a). The target information carriers are four dimensional systems with logical states $|0\rangle, |1\rangle, |2\rangle$ and $|3\rangle$. Initially and finally only the bottom two ‘qubit’ levels ($|0\rangle$ and $|1\rangle$) are populated. Controlled- X_a gates (see Equation 1 and 2) swap information between the qubit levels and the upper levels ($|2\rangle$ and $|3\rangle$), on which O does not act. In this way, conditional on the state of the control qubit, the entire quantum state of the target register is temporarily moved into an effective quantum memory on which O does not act.

Optical version of the scheme Although our technique is independent of the particular physical system and degree of freedom employed, it is particularly well suited to an optical version in terms of the polarization and spatial degrees of freedom of photonic qubits. As shown in Figure 2a, the controlled-path (CP) gate substitutes the CX_a in Figure 1b. The CP is a two-photon gate that changes the target photon’s path if the control is vertically polarized. We note that the CP gate has previously been proposed for implementing controlled gates in the context of weak optical cross-Kerr nonlinearities^{27,28}.

To understand how the CP gate works, let’s examine its structure shown in Figure 2b. Assume the inputs are two polarization-encoded photonic qubits, $\alpha|H\rangle_1 + \beta|V\rangle_1$ (control photon 1) and $\gamma|H\rangle_2 + \delta|V\rangle_2$ (target photon 2). The first PBS will convert the target state from $\gamma|H\rangle_2 + \delta|V\rangle_2$ to $\gamma|H\rangle_{2b} + \delta|V\rangle_{2r}$ where $2r$ and $2b$ denote the red and blue spatial modes of the target photon respectively. The subsequent two CNOT gates flip the polarization of the target photon if the first photon is vertically polarized. (It is assumed that if a CNOT acts on an unoccupied spatial mode the identity is enacted.) Thus, the two-photon state becomes $\alpha|H\rangle_1(\gamma|H\rangle_{2b} + \delta|V\rangle_{2r}) + \beta|V\rangle_1(\gamma|V\rangle_{2b} + \delta|H\rangle_{2r})$. Then the two spatial modes $2r$ and $2b$ of the target photon are mixed on the second PBS which converts the two-photon state to $\alpha|H\rangle_1(\gamma|H\rangle_{2r} + \delta|V\rangle_{2r}) + \beta|V\rangle_1(\gamma|V\rangle_{2b} + \delta|H\rangle_{2b})$. Finally, a half-waveplate flips the polarization in spatial mode $2b$ and thus converts the state to $\alpha|H\rangle_1(\gamma|H\rangle_{2r} + \delta|V\rangle_{2r}) + \beta|V\rangle_1(\gamma|H\rangle_{2b} + \delta|V\rangle_{2b})$: the result is that the target polarisation qubit is to be found in one of two orthogonal spatial modes, depending on the logical state of the control qubit. By defining $|H\rangle_{2b}, |V\rangle_{2b}, |H\rangle_{2r}$ and $|V\rangle_{2r}$ as $|0\rangle, |1\rangle, |2\rangle$ and $|3\rangle$ respectively, one can easily find that a CP exactly realizes the function of a CX_a gate.

Returning to Fig. 2a, suppose that the control photon is again initially in the arbitrary polarization-qubit state $\alpha|H\rangle + \beta|V\rangle$ and the target photons are initially in the multi-qubit state $|\psi\rangle$. The photons pass through a sequence of CP s which changes the path of all target photons if the control photon is vertically polarized, thus the state is converted to $\alpha|H\rangle|\psi\rangle_r + \beta|V\rangle|\psi\rangle_b$ where r and b denote the collective red

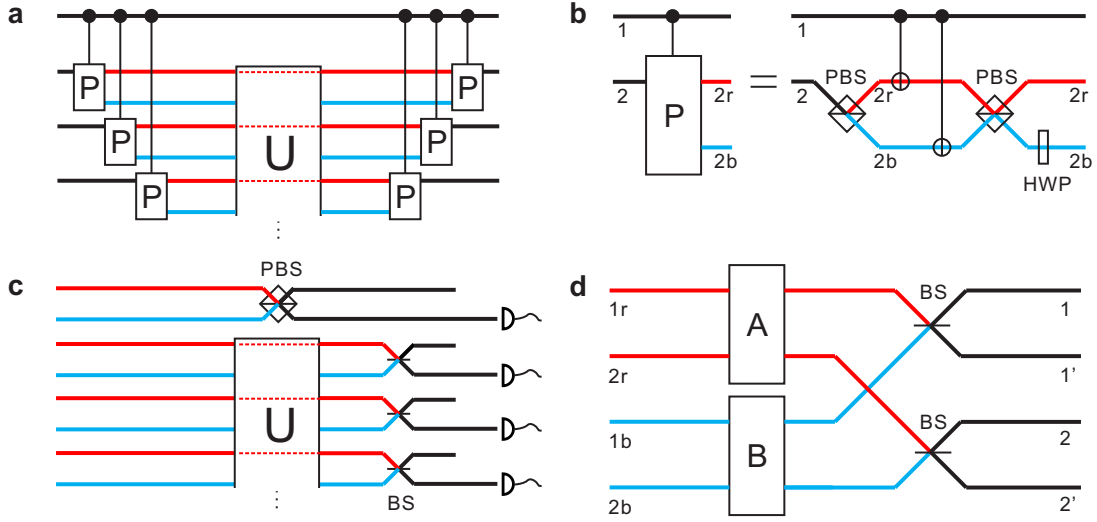


FIG. 2: **Optical implementation of the scheme.** (a) Implementation of a CU gate. The circuit is composed of three parts: controlled-path gates (CP) at the beginning, which move the target qubits from upper spatial modes (labeled red) to lower spatial modes (labeled blue) if the control qubit is in the logical state $|1\rangle$; the unitary gate U in the middle is implemented on the lower spatial modes; and CP s at the end, which combine the upper and lower spatial modes. (b) Construction of a CP gate. When the control is in the logical state $|0\rangle$, nothing is applied on the target and the photon exits in the red mode. When the control is $|1\rangle$, the polarization of the target flips and the photon exits in the blue mode. The half waveplate (HWP) flips back the polarization of the target photon in the blue mode. (c) Entanglement-based scheme. Instead of implementing CP s before the unitary gate U , one set the input state in an equal superposition of photons either all in the red modes or all in the blue modes. The CP s after U are substituted by a series of non-polarization beamsplitters (BS). (d) Linear combinations of quantum operations. The two photons are either in the red modes $1r, 2r$ or in the blue modes $1b, 2b$ which pass through quantum operations A and B respectively. Then two spatial modes $1r, 1b$ ($2r, 2b$) of photon 1 (2) are combined at a BS. By postselecting two photons at ports $1, 2$ or $1', 2'$ ($1, 2'$ or $1', 2$), one can effectively realize the quantum operation $A + B$ ($A - B$).

and blue spatial modes respectively. Next the blue spatial modes b of the target photons are acted upon by U , while the red spatial modes r do not pass through the unitary, as indicated by the dotted lines. The state is therefore converted to $\alpha|H\rangle|\psi\rangle_r + \beta|V\rangle U|\psi\rangle_b$. Finally, by repeating the sequence of CP s we obtain the desired state $\alpha|H\rangle|\psi\rangle + \beta|V\rangle U|\psi\rangle$ at the output.

There is a clear advantage over the conventional quantum computational approach to adding control qubits, in terms of the number of logic gates required. Assuming that U , which is a unitary acting on n qubits, can be decomposed into a circuit of p CNOTs and q single-qubit gates, one would use p Toffoli gates and q two-qubit controlled gates to build the corresponding CU gate, which can further be decomposed into $(3p + q)$ to $(6p + 2q)$ CNOTs and even more single-qubit gates²⁶. While $4n$ more CNOTs suffice to add a control to the n -qubit unitary U by using our method, at least $(2p + q)$ more CNOTs are needed if one sticks to the traditional scheme. For most quantum algorithm applications, such as Shor's algorithm where U is a modular exponentiation gate, the typical value of $(p + q)$ is about $72n^3$ which is on the order of $O(n^3)$ and thus $(2p + q)$ is much larger than $4n$ when n becomes large^{29,30}. Furthermore, if U is a non-unitary operation then the conventional approach is to rewrite this as a unitary on a larger Hilbert space, at a significant cost to the number of gates required. There is no additional cost to add controls to non-unitary operations following our approach.

Entanglement-based scheme Even a two-qubit demonstration of our scheme would require two CP gates and subse-

quently four CNOT gates, which is presently out of reach using current linear-optical quantum information processing technology. However, the effect of the CP gate is to generate entanglement between the control qubit and target register, and this kind of entanglement can be generated directly from existing photon sources. We now present an alternative entanglement-based version of our scheme which is feasible with current technology.

Consider the optical circuit schematic shown in Figure 2c. At the input a spatially-entangled n -photon state is injected that is an equal superposition of finding one photon in each of the n red modes and one photon in each of the n blue modes. In the case where the polarization of the n -photon input state is $|\phi\rangle = (\alpha|H\rangle + \beta|V\rangle)|\psi\rangle$, where $\alpha|H\rangle + \beta|V\rangle$ is the upper control qubit and $|\psi\rangle$ is the joint state of the lower $(n-1)$ target register qubits, then the initial state can be written as

$$\frac{1}{\sqrt{2}}(|\phi\rangle_r |vac\rangle_b^{\otimes n} + |vac\rangle_r^{\otimes n} |\phi\rangle_b) \quad (3)$$

where r and b label the collective red and blue spatial modes respectively, and $|vac\rangle$ represents an unoccupied mode. From now on we will drop the unoccupied vacuum modes from the notation. Note that, as we will show, it is possible to create such a state from a spontaneous parametric down conversion photon source. The quantum operation U acts only on photons in the blue spatial modes of the target register. The information about whether the target state ψ does or does not undergo the operation U is therefore encoded in the spatial mode of the control photon. Mixing the two control modes on a polarizing beamsplitter (PBS) and post-selecting

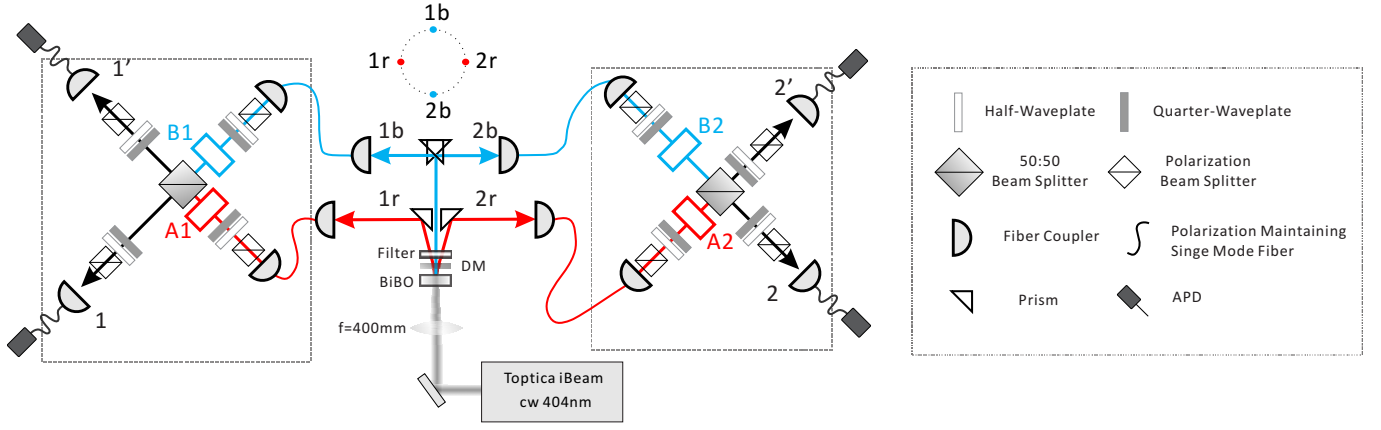


FIG. 3: **Experimental setup for realizing CU gates.** A 60 mW continuous-wave (CW) laser beam with a central wavelength of 404nm is focused onto a BiBO crystal to create photon-pairs. Both the horizontal (modes 1r and 2r) and vertical (modes 1b and 2b) photon pairs are collected. Prior to collection into polarization-maintaining fibers (PMF), the photons are spectrally filtered by narrow-band filters ($\Delta\lambda_{FWHM} = 3.2$ nm). A1, B1, A2 and B2 are four single-qubit gates. By post-selecting the case the two photons exit at ports 1 and 2, one would effectively realize a two-qubit quantum gate ($A1 \otimes A2 + B1 \otimes B2$). The phase between the two components is stabilized by monitoring the coincidence count rates between detectors 1' and 2'.

on finding the control photon in the lower spatial mode moves this information into the polarization of the control photon, yielding the state:

$$\frac{1}{\sqrt{2}}(\alpha|H\rangle|\psi\rangle_r + \beta|V\rangle|U\rangle|\psi\rangle_b) \quad (4)$$

Finally, the red and blue modes of each target qubit are mixed on non-polarising beamsplitters (BS) to remove the path information. In the case where all photons exit in the lower paths, the output state is

$$\frac{1}{\sqrt{2^n}}(\alpha|H\rangle|\psi\rangle + \beta|V\rangle|U\rangle|\psi\rangle) \quad (5)$$

as required. The probability of success is $(1/2)^n$, however all combinations of the control photon arriving in lower spatial mode and an even number of target photons arriving in lower spatial modes will give a state with the same form as in Eq.5. There are 2^{n-2} such combinations so the total probability of success is 1/4, regardless of the number of qubits U acts on. The important feature of our approach — that any operation (known or unknown) can be controlled without changing the way the operation is done — is retained in the entanglement based approach.

This approach can be reformulated in a more general way as shown in Figure 2d. Here we consider the two-photon case for simplicity. Beginning with the two photon input state of Equation 3, the red and blue modes pass through quantum operations A and B respectively. The state $\frac{1}{\sqrt{2}}(A|\phi\rangle_r + B|\phi\rangle_b)$ is obtained. After mixing the spatial modes on the two BSs, one would get $(A + B)|\phi\rangle$ if the two photons exit at ports 1 and 2 or 1' and 2'. Otherwise, if the two photons exit at ports 1 and 2' or 1' and 2, $(A - B)|\phi\rangle$ would be obtained. To realize the CU gate, one just needs to set $A = |H\rangle\langle H| \otimes I$ and $B = |V\rangle\langle V| \otimes U$, where $|H\rangle\langle H|$ and $|V\rangle\langle V|$ denote projectors onto $|H\rangle$ and $|V\rangle$ respectively.

This approach provides a new perspective on constructing quantum gates: While the traditional decomposition method

can be regarded as performing multiplication, which corresponds to rewriting the target gate matrix as the product of several gate matrices, our method is performing linear combination which means rewriting the target gate matrix as the sum of several gate matrices. This entanglement-based scheme would be useful for small scale applications as well as subroutines in larger calculations, and could be made deterministic following the original prescription for linear optical quantum computation³¹. Introducing non-linearities is another way to approach a unit success probability²⁷.

Experimental demonstration We now present experimental demonstrations of several two-qubit CU gates using this general entanglement-based method (specifically corresponds to Figure 2d). Figure 3 shows a schematic diagram of our experiment. Note the simplicity of this scheme relative to the previous demonstration of photonic CU gates²⁶, in particular the fact that it requires no quantum interference. A continuous-wave laser is focused onto a BiBO crystal and thus produces photon pairs through the type-I spontaneous parametric-down conversion (SPDC) process. We collect two photons from four points from the SPDC cone, as shown, resulting in a two-photon four-mode state³² of the form $\frac{1}{\sqrt{2}}(|H\rangle_{1r}|H\rangle_{2r} + |H\rangle_{1b}|H\rangle_{2b})$. By passing each mode through several waveplates, we prepare a state $\frac{1}{\sqrt{2}}(|\phi\rangle_{1r,2r} + |\phi\rangle_{1b,2b})$, where $|\phi\rangle$ can be an arbitrary two-qubit separable state. Here we designate photon 1 as the control, which is in modes 1r and 1b, and photon 2 as the target, which is in modes 2r and 2b. Before modes 1r (2r) and 1b (2b) are combined at a BS, we let the four modes pass through four single-qubit gates A1, B1, A2 and B2 which are constructed from waveplates or PBSs. Then, by measuring the two-photon coincidences between detectors at ports 1 and 2, we get the state $(A + B)|\phi\rangle$, where $A = A1 \otimes A2$ and $B = B1 \otimes B2$. As explained above, by setting $A1 = |H\rangle\langle H|$, $A2 = I$, $B1 = |V\rangle\langle V|$ and $B2 = U$, the corresponding CU gate is obtained.

We constructed a series of CU gates, including CNOT, C-

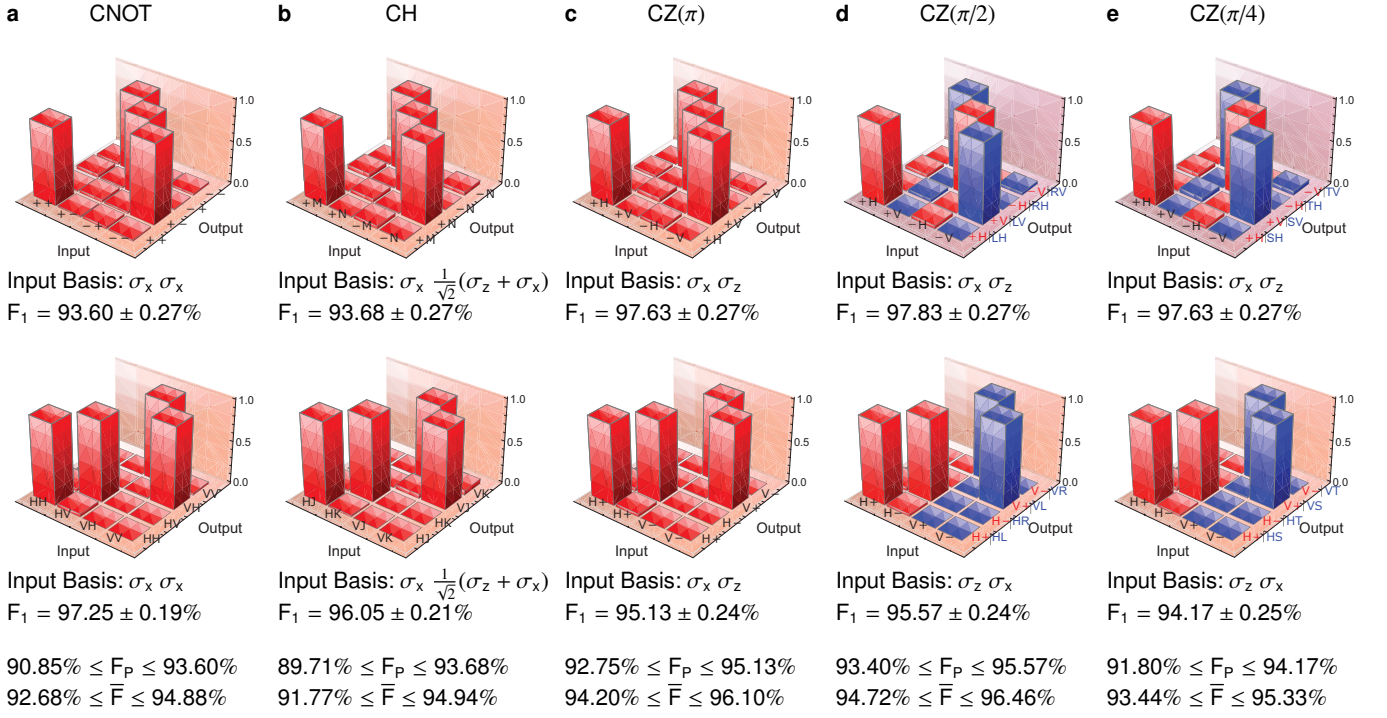


FIG. 4: **Implementing two-qubit controlled-unitary operations by harnessing entanglement in a larger Hilbert space.** (a–e) Experimentally measured “truth tables” for several CU gates. For the inputs of the CH gate $|M\rangle$ and $|N\rangle$ ($|J\rangle$ and $|K\rangle$) are the eigenstates of $\frac{1}{\sqrt{2}}(\sigma_z + \sigma_x)$ ($\frac{1}{\sqrt{2}}(\sigma_z - \sigma_x)$) with $+1$ and -1 eigenvalues respectively: *i.e.* $|M\rangle = \cos(\pi/8)|H\rangle + \sin(\pi/8)|V\rangle$; $|N\rangle = \sin(\pi/8)|H\rangle - \cos(\pi/8)|V\rangle$; $|J\rangle = \cos(5\pi/8)|H\rangle + \sin(5\pi/8)|V\rangle$; $|K\rangle = \sin(5\pi/8)|H\rangle - \cos(5\pi/8)|V\rangle$. Notice that two different output measurement bases are applied for each truth table of CPhase($\pi/2$) and CPhase($\pi/4$). The red columns correspond to red output labels while the blue columns correspond to blue output labels which include states such as $|HL\rangle$, $|HR\rangle$, $|HS\rangle$ and $|HT\rangle$ where $|R/L\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$ and $|T/S\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm e^{i\pi/4}|V\rangle)$. Bounds on the process fidelities F_p and average fidelities \bar{F} are calculated from the classical fidelities shown under the truth tables. Each truth table requires 16 measurements and each measurement is taken 1 s. The count of each high column is around 2000. Note that for probabilities near zero values in the truth tables we increased the integration time from 1 s to 10 s in order to improve the statistics.

Hadamard (CH), CPhase (CZ), CZ($\pi/2$) and CZ($\pi/4$) gate, by setting $B2 = X, H, Z, Z_{\pi/2}$ and $Z_{\pi/4}$, respectively. To evaluate the performance of these gates, we adopted the method introduced in ref. 33. For each gate, two truth tables are measured in complimentary bases. The bases we chose are shown in Figure 4. The fidelity of these truth tables with the ideal (F_1 and F_2) bound the process fidelity of the gate via:

$$(F_1 + F_2 - 1) \leq F_p \leq \min(F_1, F_2) \quad (6)$$

We have also performed full process tomography on one of these gates (see Methods section). From F_p we can calculate the output state fidelity averaged over all input states via the average gate fidelity:

$$\bar{F} = \frac{dF_p + 1}{d + 1}, \quad (7)$$

where d is the dimension of the gate ($d = 4$ for a two-qubit gate). The results are shown in Figure 4.

This method is not limited to realizing CU gates. By changing the values of $A1$, $A2$, $B1$, and $B2$, one can implement various two-qubit quantum operations. For example, by setting $A1 = A2 = |H\rangle\langle H|$ and $B1 = B2 = |V\rangle\langle V|$, one can realize a very useful quantum gate known as entanglement filter (EF)^{34,35}. An EF is a special (non-unitary) quantum gate

which filters multi-qubit states on the basis of correlations. Here, our two-photon EF transmits photon pairs only if they share the same horizontal or vertical polarization, without measuring the polarization state. Compared with the previous method^{34,35}, our method is simpler and more intuitive. We implement this two-photon EF using the setup shown in Figure 3 where $A1 = A2 = |H\rangle\langle H|$ and $B1 = B2 = |V\rangle\langle V|$ and the results are shown in Figure 5a.

Another interesting feature of our approach is that the method of realizing a quantum gate is not unique: one can choose different sets of A and B to get the same $A + B$. Take the two-photon EF for example, we can realize it in another way by setting $A1 = A2 = I$ and $B1 = B2 = Z$. This can be verified by comparing the matrix of $I \otimes I + Z \otimes Z$ with $|H\rangle\langle H| \otimes |H\rangle\langle H| + |V\rangle\langle V| \otimes |V\rangle\langle V|$ which are equivalent up to a constant of order unity. Unlike the first way of realizing an EF, one does not use any projection but only unitary operators which means that in fact no components are filtered out: While the $|H\rangle|H\rangle$ and $|V\rangle|V\rangle$ components would exit at 1 and 2 or 1' and 2' which corresponds to realizing the quantum gate $A + B$, the $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ components would exit at 1 and 2' or 1' and 2 which corresponds to realizing $A - B$. As the $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ components are not filtered out in this case, we call the device an entanglement splitter (ES). The

ES operation is deterministic and the experimental data from this gate are shown in Figure 5b & c.

Interestingly, the mechanics of the *ES* can be understood in a different way. The following equations always hold

$$\begin{aligned} Z \otimes Z(I \otimes I + Z \otimes Z)|\phi\rangle &= +(I \otimes I + Z \otimes Z)|\phi\rangle \\ Z \otimes Z(I \otimes I - Z \otimes Z)|\phi\rangle &= -(I \otimes I - Z \otimes Z)|\phi\rangle \end{aligned} \quad (8)$$

which means $(I \otimes I + Z \otimes Z)|\phi\rangle$ (or $(I \otimes I - Z \otimes Z)|\phi\rangle$) is always the eigenstate of operator $Z \otimes Z$ with eigenvalue +1 (or -1) no matter what the two-qubit state $|\phi\rangle$ is. Then one can deduce that $I \otimes I + Z \otimes Z$ (or $I \otimes I - Z \otimes Z$) must be a projector which projects any input state to the eigenstate of $Z \otimes Z$ with eigenvalue +1 (or -1). As our circuit realizes $I \otimes I + Z \otimes Z$ and $I \otimes I - Z \otimes Z$ simultaneously, it can be regarded as an eigenstate generator of, or eigenvalue measuring device for, operator $Z \otimes Z$. One can easily find the above reasoning would hold when replacing $Z \otimes Z$ with any two-qubit operator W which fulfill $W^2 = I \otimes I$. This example nicely illustrates the power of linear combination of quantum gates. Although an alternative implementation of an *EF* has previously been reported³⁵, the *ES* has not been realized; as far as we know, our method is the only solution for constructing these kinds of entangling gates.

The imperfections of our experimental results are mainly due to three effects. First, the photons generated in the SPDC source are not completely indistinguishable; second, the phase between the two spatial modes is not perfectly stabilized (to zero); third, the optical components are not perfectly set to the desired values (e.g. waveplates' angles). For the *EF* experiment, $A1$, $B1$, $A2$ and $B2$ are all projectors and implemented with PBS. In this case the $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ components are nearly completely filtered out and this is not affected by phase errors between the two spatial modes. However in the *ES* experiment, no component is filtered out, the suppression of $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ is all based on interference, which is very sensitive to phase errors between the two spatial modes. The implementation of the *CU* gates is in between of the two previous cases, where $A1$, $B1$ are projectors and $A2$, $B2$ are unitaries. This explains why the fidelity values of the *CU* gates are higher than those of the *ES* and lower than those of the *EF*.

Discussion

Our method will allow simplification of small scale linear optical circuits. For example, the CNOT gate (or other entangling gates) demonstrated above could be combined with a post-selected version of the same gate to perform a sequence of two entangling gates on two photonic qubits. This would require two photons rather than four — which would normally be required for the first gate to be heralded. This type of approach is likely to be of great benefit in circuits of up to 6-10 photons where the appropriate entangled states can be generated³² and one can rely on inefficient measurement.

This new approach to realizing quantum circuits also enables a quantum state to control the implementation of a quantum gate, thereby opening up the possibility to have truly quantum inputs to quantum information processors. As shown

in Fig. 2a, if we set the control to be $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and let the red and blue spatial modes of the target pass through gate O_1 and O_2 instead of I and U respectively, where O_1 and O_2 represent two arbitrary quantum gates, the output state would be $\frac{1}{\sqrt{2}}(|0\rangle O_1 |\psi\rangle + |1\rangle O_2 |\psi\rangle) = \frac{1}{\sqrt{2}}(|0\rangle O_1 + |1\rangle O_2) |\psi\rangle$, where $|\psi\rangle$ is the initial target state. In some sense, our circuit realizes a peculiar entangled “state” $\frac{1}{\sqrt{2}}(|0\rangle O_1 + |1\rangle O_2)$ in which a quantum bit and a quantum gate are entangled (without needing to know what the gate is). This peculiar entanglement connecting a qubit with quantum gates may have some useful implications. An immediate application is to teleport a qubit onto a quantum gate by using this entangled “state”. In this sense, one can get a quantum gate $\alpha O_1 + \beta O_2$ by teleporting a qubit $\alpha|0\rangle + \beta|1\rangle$. This is a novel way to control a quantum gate by using a quantum bit that is related to ideas of programmable quantum gate arrays³⁶.

In summary, we have proposed a different approach to realizing the controlled operations that are at the heart of the majority of important quantum algorithms. With this method, one can directly integrate an arbitrary operation into the circuit to build the corresponding *CU* gate even if the unitary U is unknown. This is in contrast to other methods that harness extra degrees of freedom^{26,37} that work only for known single target qubit unitaries. Our method is not limited to *CU* gates but can be extended to realize more general entangling gates. We demonstrated the power of this approach by experimentally implementing several high-fidelity two-qubit gates. In each case the implementation of the control circuit was completely independent of the choice of quantum operation. This method has the potential to change the way we implement quantum circuits for all algorithms and will find a wide range of applications across quantum information science and technology as the complexity of the quantum circuits implemented grows to include more sophisticated algorithms.

Methods

An alternative experimental demonstration In the experiments described in the main text, we prepared the spatial entangled state $\frac{1}{\sqrt{2}}(|\phi\rangle_{1r,2r} + |\phi\rangle_{1b,2b})$ as the input (see Figure 3) for implementing the various two-qubit quantum gates, where $|\phi\rangle$ is an arbitrary polarization-encoded two-qubit separable state. Here we want to point out that the phase between the two components $|\phi\rangle_{1r,2r}$ and $|\phi\rangle_{1b,2b}$ was stabilized by using monitoring and feedback method. Although the phase stabilizing approach is good enough to construct these quantum gates, for application such as phase estimation algorithm, where phase itself is the target to be measured, a setup with inherent phase stability is required.

Here we present an experimental demonstration of the same scheme by using a setup which is inherently phase stable. Instead of using type-I spontaneous parametric down-conversion (SPDC) source to get the spatial entangled photon pairs, we use type-II SPDC source to get polarization entangled photon pairs first and then convert them to the spatial entangled ones. In this way, we can build a displaced-Sagnac structure in the setup to make the phase stable. Figure 6 shows the schematic diagram of our experiment. We use the same continuous wave laser to pump a BBO crystal cut for type-II SPDC and get the two photon state $\frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2)$.

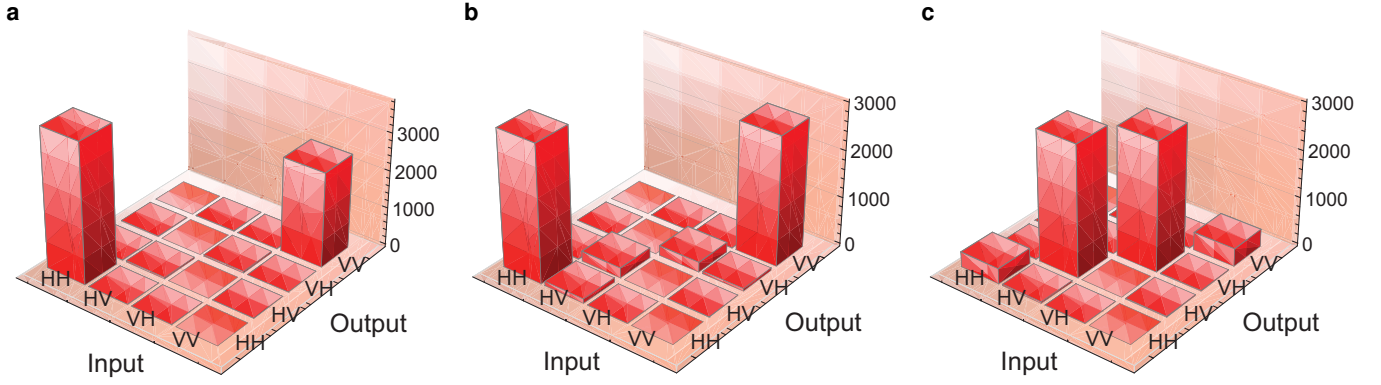


FIG. 5: **An entanglement filter and entanglement splitter.** (a) Logical basis truth table for an entanglement filter; the classical fidelity is $98.03 \pm 0.17\%$. (b,c) Logical truth tables for the entanglement splitter. The entanglement splitter's two outputs correspond to two complementary entanglement filters: one transmits $|HH\rangle$ and $|VV\rangle$ components (b); and the other transmits $|HV\rangle$ and $|VH\rangle$ components whose truth table is shown in (c); their classical fidelities in H/V basis are $90.27 \pm 0.37\%$ and $87.38 \pm 0.42\%$ respectively. Here the classical fidelity is defined as the ratio of correctly transmitted photon pairs to the total number of transmitted photon pairs. The data of each column corresponds to 1 s of measurement.

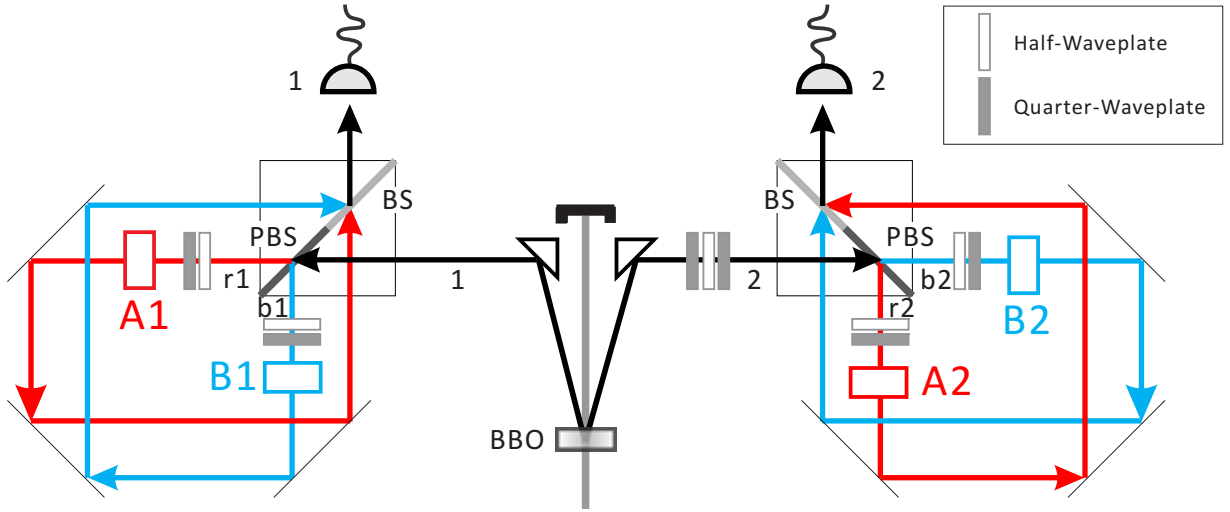


FIG. 6: **Experimental setup in a Sagnac structure.** A 60 mW continuous-wave (CW) laser beam with a central wavelength of 404nm is focused onto a type-II BBO crystal to create entangled photon-pairs. The PBS part of the cubes convert the polarization-entangled state to spatial-entangled state. A1, B1, A2 and B2 are four single-qubit gates. By post-selecting the case where the two photons exit at ports 1 and 2, one would effectively realize a two-qubit quantum gate ($A1 \otimes A2 + B1 \otimes B2$). The displaced-Sagnac structure makes the phase between modes $r1$ and $b1$ ($r2$ and $b2$) inherently stable.

By placing PBS/BS cubes (half PBS, half BS) on both arms and letting the photons pass through the PBS part of the cubes, we would get the state $\frac{1}{\sqrt{2}}(|H\rangle_{1r}|V\rangle_{2r} + |V\rangle_{1b}|H\rangle_{2b})$. The HWP and QWP on each path further convert the state to $\frac{1}{\sqrt{2}}(|\phi\rangle_{1r,2r} + |\phi\rangle_{1b,2b})$ which is exactly same as the spatial entangled state in the original experiments. We let the four spatial modes $1r$, $2r$, $1b$ and $2b$ pass through four single-qubit gates A1, A2, B1 and B2 respectively and then mix the spatial modes $1r$ and $2r$ ($1b$ and $2b$) on the BS part of the cube. By postselecting the case when two photons exit at ports 1 and 2, the quantum operation $A + B$ is obtained. Here we set $A1 = |H\rangle\langle H|$, $B1 = |V\rangle\langle V|$, $A2 = I$, $B2 = X$ and thus realize a CNOT gate.

As the phase θ between r and b modes is inherently stable in our setup, we can now show the variation of the coincidence rates with the phase θ change. By setting $|\phi\rangle$ to be $|+\rangle|H\rangle$, the state $\frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)$ would be obtained. We then place a set of waveplates (QWP, HWP and QWP) in the path of photon 2 as shown to continuously tune the phase between the spatial modes r and b and measure the

$|+\rangle|+\rangle$ and $|+\rangle|-\rangle$ two-photon coincidence rates at the output, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. As shown in Figure 7, two complementary cosine curves are obtained as expected.

We fully characterize the CNOT gate through quantum process tomography (QPT) and the experimentally reconstructed process matrices are shown in Figure 8. We observe a high process fidelity of $96.13 \pm 0.17\%$ with the ideal case.

Acknowledgments

We thank P. J. Shadbolt for writing the code for reconstructing the process matrix and H. F. Hofmann, A. Laing, J. C. F. Matthews, A. Politi for helpful discussions. This work was supported by ERC, EPSRC, PHORBITECH, NOKIA, IARPA, the Leverhulme Trust, and NSQI. J.L.O'B. acknowledges a Royal Society Wolfson Merit Award.

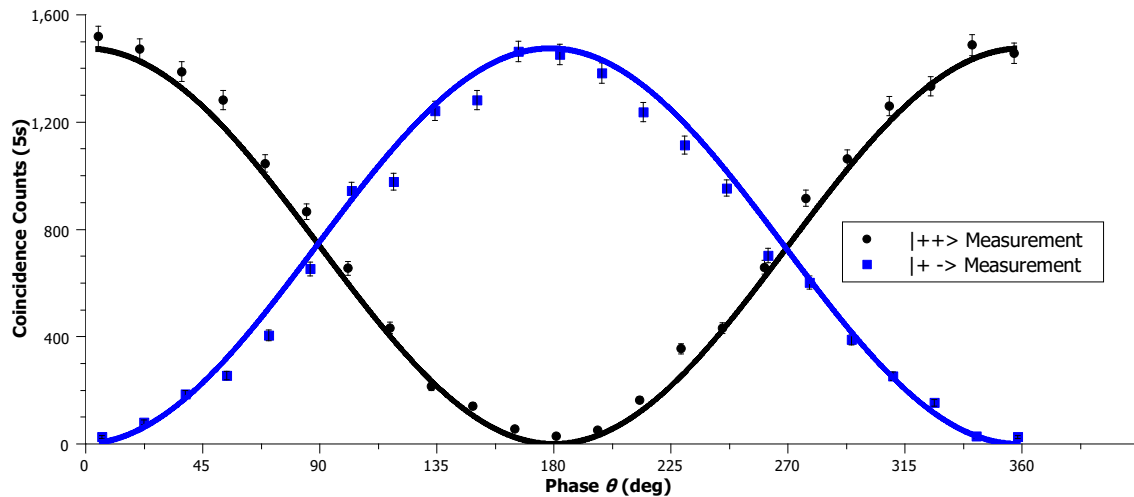


FIG. 7: Coincidence rates as a function of the phase between spatial modes r and b . The two-photon output state would be $\frac{1}{\sqrt{2}}(|H\rangle_{1r}|V\rangle_{2r} + e^{i\theta}|V\rangle_{1b}|H\rangle_{2b})$, where θ is the relative phase between spatial modes r and b . The coincidence rates of $|+\rangle|+\rangle$ (or $|+\rangle|-\rangle$) would be $C(1 + \cos \theta)/2$ (or $C(1 - \cos \theta)/2$) where C is the maximum count rate of $|+\rangle|+\rangle$ (or $|+\rangle|-\rangle$).

-
- * Electronic address: Jeremy.O'Brien@bristol.ac.uk
- ¹ N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
 - ² L. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
 - ³ P. W. Shor, Proc. 35th Annu. Symp. Foundations of Computer Science and IEEE Computer Society and Los Alamitos and CA pp. 124–134 (1994), ed. S. Goldwasser.
 - ⁴ R. P. Feynman, *Int. J. Thy. Phys.* **21**, 467 (1982).
 - ⁵ M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
 - ⁶ T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, *Nature* **464**, 45 (2010).
 - ⁷ F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt, *Nature* **422**, 408 (2003).
 - ⁸ D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, et al., *Nature* **422**, 412 (2003).
 - ⁹ T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A* **68**, 032316 (2003).
 - ¹⁰ J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, *Nature* **426**, 264 (2003).
 - ¹¹ S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, *Phys. Rev. Lett.* **93**, 020504 (2004).
 - ¹² X.-H. Bao, T.-Y. Chen, Q. Zhang, J. Yang, H. Zhang, T. Yang, and J.-W. Pan, *Phys. Rev. Lett.* **98**, 170502 (2007).
 - ¹³ W.-B. Gao, P. Xu, X.-C. Yao, O. Gühne, A. Cabello, C.-Y. Lu, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Phys. Rev. Lett.* **104**, 020501 (2010).
 - ¹⁴ M. Steffen, M. Ansmann, R. C. Bialczak, N. Katz, E. Lucero, R. McDermott, M. Neeley, E. M. Weig, A. N. Cleland, and J. M. Martinis, *Science* **313**, 1423 (2006).
 - ¹⁵ J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij, *Nature* **447**, 836 (2007).
 - ¹⁶ O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch, *Nature* **425**, 937 (2003).
 - ¹⁷ M. Anderlini, P. J. Lee, B. L. Brown, J. Sebby-Strabley, W. D. Phillips, and J. V. Porto, *Nature* **448**, 452 (2007).
 - ¹⁸ B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, *Phys. Rev. Lett.* **99**, 250505 (2007).
 - ¹⁹ C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, *Phys. Rev. Lett.* **99**, 250504 (2007).
 - ²⁰ A. Politi, J. C. F. Matthews, and J. L. O'Brien, *Science* **325**, 1221 (2009).
 - ²¹ B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, et al., *Nature Chem.* **2**, 106 (2010).
 - ²² A. Kitaev, A. Shen, A. Shen, M. Vyalyi, and M. Vyalyi, *Classical and quantum computation* (Amer Mathematical Society, 2002).
 - ²³ A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, *Science* **309**, 1704 (2005).
 - ²⁴ R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
 - ²⁵ P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, *Nature* **434**, 169 (2005).
 - ²⁶ B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, *Nat. Phys.* **5**, 134 (2009).
 - ²⁷ Q. Lin and B. He, *Phys. Rev. A* **80**, 042310 (2009).
 - ²⁸ Q. Lin, B. He, J. A. Bergou, and Y. Ren, *Phys. Rev. A* **80**, 042311 (2009).
 - ²⁹ V. Vedral, A. Barenco, and A. Ekert, *Phys. Rev. A* **54**, 147 (1996).
 - ³⁰ D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, *Phys. Rev. A* **54**, 1034 (1996).
 - ³¹ E. Knill, R. Laflamme, and G. J. Milburn, *Nature* **409**, 46 (2001).
 - ³² A. Rossi, G. Vallone, A. Chiuri, F. De Martini, and P. Mataloni, *Phys. Rev. Lett.* **102**, 153902 (2009).
 - ³³ H. F. Hofmann, *Phys. Rev. Lett.* **94**, 160504 (2005).
 - ³⁴ H. F. Hofmann and S. Takeuchi, *Phys. Rev. Lett.* **88**, 147901 (2002).
 - ³⁵ R. Okamoto, J. L. O'Brien, H. F. Hofmann, T. Nagata, K. Sasaki, and S. Takeuchi, *Science* **323**, 483 (2009).
 - ³⁶ M. A. Nielsen and I. L. Chuang, *Phys. Rev. Lett.* **79**, 321 (1997).
 - ³⁷ T. C. Ralph, K. J. Resch, and A. Gilchrist, *Phys. Rev. A* **75**,

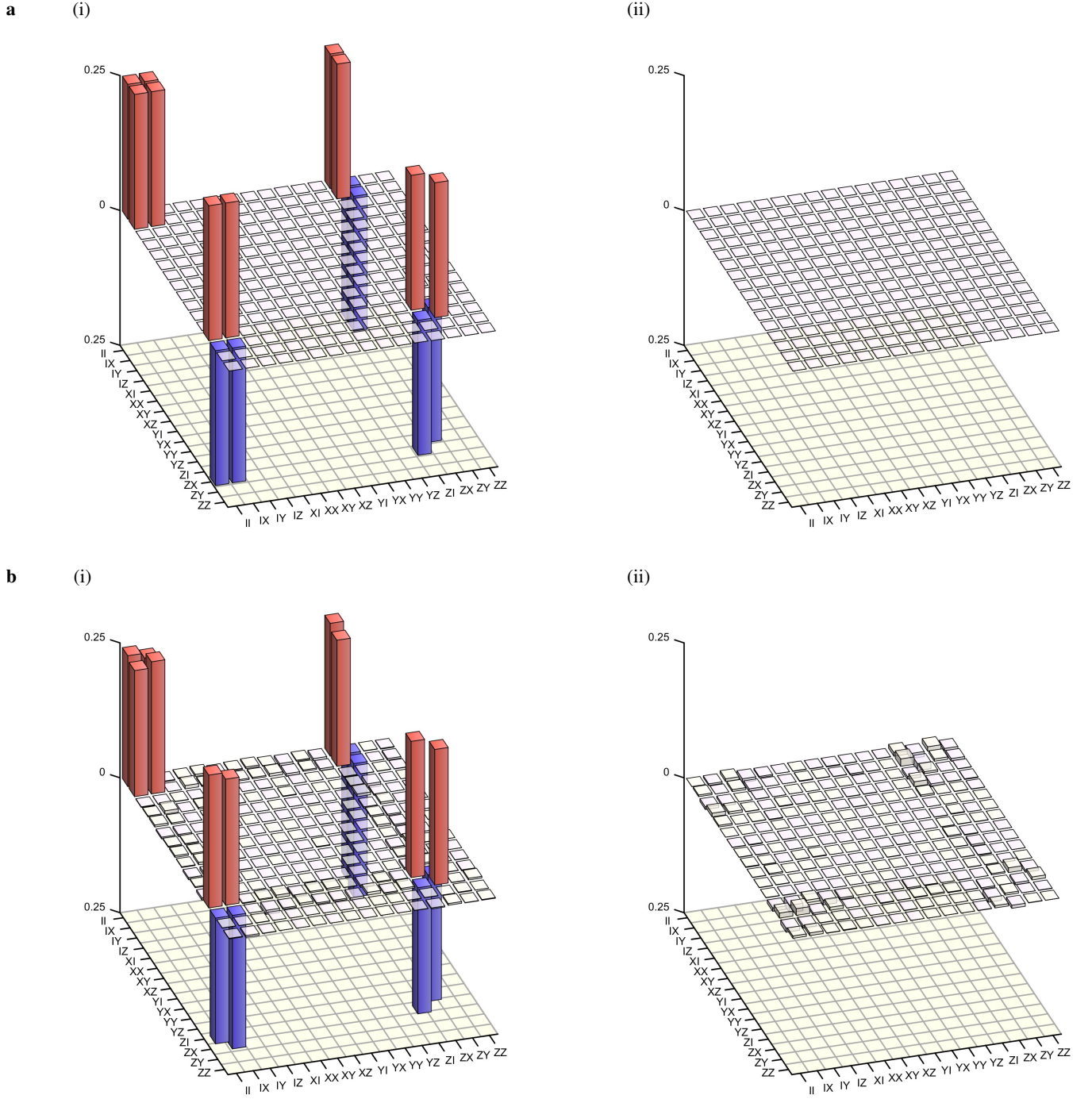


FIG. 8: **Process matrix of the CNOT gate** (a) Ideal process matrix. (b) Maximum-likelihood experimental reconstructed process matrix. (i) Real and (ii) imaginary parts are shown. We observe a high process fidelity of $96.13 \pm 0.17\%$ with the ideal case. The error estimate is obtained by performing many reconstructions with random noise added to the raw data in each case. Matrices are presented in the standard Pauli basis.³⁸

022313 (2007).

080502 (2004).

³⁸ J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, Phys. Rev. Lett. **93**,